BB84 algorithm for cryptographic keys distribution

September 2010

Introduction

Two communications channels are in use, both of them are insecure, one is classic and another quantum. The quantum channel is an optical fiber (or equivalent) where photos travels one by one. The classic channel can be Internet, phone or any other communication system.

Alice sends the photos to Bob one by one, polarized vertically, horizontally or in diagonal (45º or 135º) in a random way. Bob is going to measure them to discover what was their polarization using two set of basis.

Basis definition

Basis A $|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Basis B $|+\rangle = |\uparrow\rangle + |\downarrow\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ $|-\rangle = |\uparrow\rangle - |\downarrow\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

Coding criteria

$false_A = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $true_A = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$false_B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ $true_B = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

Measurement probabilities of every encoded state

	read *false* using basis *A*	read *true* using basis *A*	read *false* using basis *B*	read *true* using basis *B*
Encode *false* using basis *A*	**100%**	0%	50%	50%
Encode *true* using basis *A*	0%	**100%**	50%	50%
Encode *false* using basis *B*	50%	50%	**100%**	0%
Encode *true* using basis *B*	50%	50%	0%	**100%**

Generation phase: Step 1, qubits transmission

The *master* station chooses a basis randomly, and a value `true` or `false` also randomly. Those two classical values are stored. It sends the quantum state of encoding the `true` or `false` value in the selected basis.

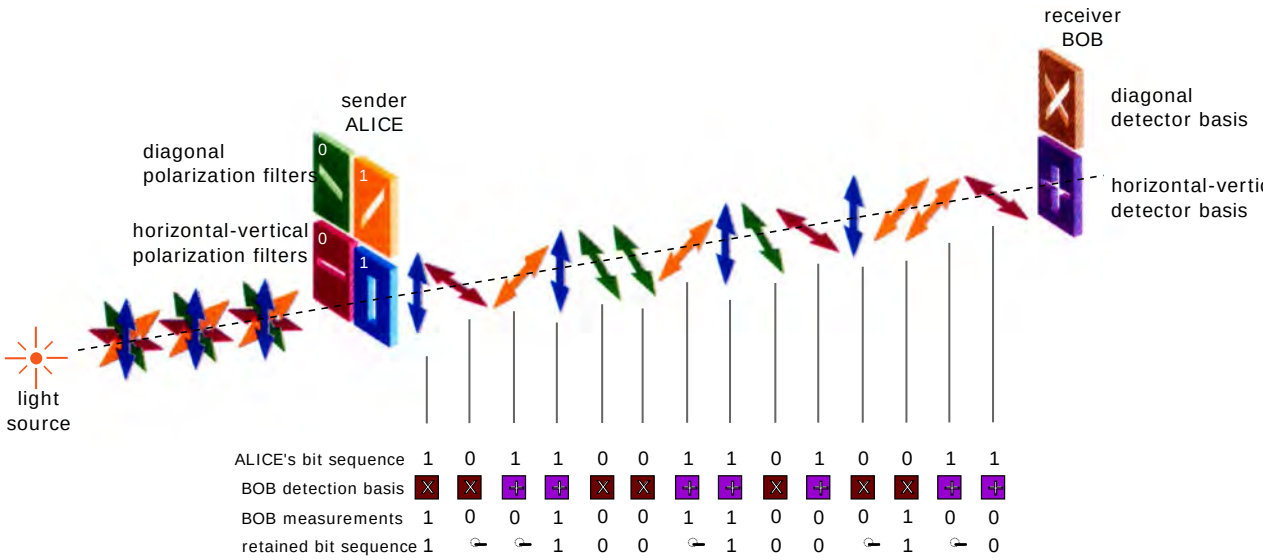
The *slave* station measures the quantum states using randomly selected basis. It stores the used basis and measured value.

The *master* station must send $(4 + \delta) N$ qubits. Being N the size of the key to generate, and δ a parameter related to the specific quantum channel. This parameter is related with the noise level or fidelity of the channel.

Generation phase: Step 2, basis transmission

The *master* station sends the basis used to encoding the data, and the *slave* store them.

It does not sends under any reason the data has been used to generate the qubits. Those are secret values that are waiting to be be transmitted



Generation phase: Step 3, transmission of coincidences

The *slave* station sends the positions that performed a correct measurement. The *slave* station does not sends what measured in the first step of this phase. This is the secret to transmit, and must be kept secret.

Verification of transmitted key size

This phase checks the size of the intermediary key just generated. It should have a minimum size of $2N$, being N the size of the data to cypher. This is the reason of the mysterious 4 that appeared in the first phase of the algorithm. How the success rate of measuring in an unknown base is $\frac{1}{2}$, and we ignore the invalid ones, at the end of the first phase only half of the sent values remains. So, if we want to receive $2N$ values, we should send at least $4N$.

However it also exists the possibility, but small, of not granting the minimum size, (this is configurable with the δ parameter), in this case the BB84 key distribution is aborted. Several attempts of establishing a valid key will be done before concluding that the channel is broken or there is a spy (will be explained later).

We have an intermediary key of size $Z \geq 2N$. We transmit the exceeding $Z - N$ (at lest they will be N) for ensuring the integrity of the transmission of the first step of the previous phase (transmission of quantum states).

Checking phase: Step 1, transmission of positions to check

The *master* stations transmit the positions to check, and the *slave* station stores them.

Checking phase: Step 2, master station transmit the values

In this step the *master* station and the *slave* station already know what bits are going to be compared. The *master* one sends the values that wanted to transmit, and the *slave* store them.

Checking phase: Step 3, slave station transmit the values

In this step the *slave* station will send what has received and measured in the correct basis during the generation step. In this way the *master* station will be able to calculate the noise level of the channel.

Decision phase

Now the *master* and the *slave* station have enough information to determine the noise level that happened during the data transmission. Both have what was intended to be sent, and what was received in reality. If the noise level is above certain level, the transmission is canceled.